Application No.: 09/446,525   Docket No.: 20162-00540-US

REMARKS

Claims 14-49 are pending in the application. Favorable reconsideration of the application is requested.

Withdrawal of the objection to claim 17 is requested in light of the amendments made hereto.

Withdrawal of the objection of claim 39 as being in improper multiple dependent form is requested. The claim has been amended so that it depends from the appropriate claim.

Withdrawal of the rejection of claim 49 under 35 U.S.C. § 112, is requested in light of the amendments made herein.

Withdrawal of the rejection of claims 14-27 and 40 under 35 U.S.C. § 103 as being unpatentable over DES (Data Encryption Standard), National Bureau of Standards (U.S.), in view of Matsui (New Block Encryption Algorithm MISTY), is requested. As noted in the Office Action, the primary reference DES fails to disclose any second nonlinear transformation part.

The Matsui reference describes a type or encryption system known as MISTY 1 and MISTY 2. According to the reference, a 64-bit data block is divided into a left 32-bit data block and a right 32-bit data block. The left 32-bit data block is transformed in each of the plurality of round processing stages to be transformed by an FO-function, and that result is XORed with the right 32-bit data block. The XORed output and the right 32-bit data block are switched with each other. The 32-bit block data from both the left and right are then input to a subsequent round processing stage. The FO function in each round processing stage is constructed as a double nestled three round process, shown in Fig. 4, and the block size of data supplied to each of the s-functions in the lowest level is only 9-bits which allows the use of nonlinear transformers (I.E., s-functions) of a smaller size while achieving a higher robustness.

14

Application No.: 09/446,525   Docket No.: 20162-00540-US

According to Fig. 4, since each FO-function is a k-nestled 3-round processing stage, the total number of s-functions in series becomes 3^k times as many as the case in which each FO-function is a single s-function. Encryption processing speed is roughly inversely proportional to the number of s-functions in series, which means that the MISTY1 and MISTY 2 encryption schemes have a lower encryption processing speed.

This is to be distinguished from the present invention. According to the present invention, the entire bits of a block data supplied to each nonlinear function part, such as 304 in Fig. 3, is subjected to nonlinear processing by first and second nonlinear transformation parts such as 343-346 and 348-351 in Fig. 4, and as set forth in rejected claim 14. Accordingly, the total number of cascade processing stages for nonlinear transformation parts in the cascade-connected round processing parts 38_0-38_{n-1} is two times the number of round processing parts and therefore encryption processing speed is much faster than in the MISTY devices. The data input to each nonlinear function part such as 304 is split by a splitting part such as 342 into plural bit springs and individually processed by a plurality of first nonlinear transformation parts such as 343-346. The cryptographic process according to the present invention can be easily adapted to encrypt input data in an increased length without lowering the processing speed. This feature cannot be obtained from the MISTY 1 or 2 systems.

It is clear, that the present invention as defined by claim 14 is not suggested by the combination of DES and Matsui. As noted above, numerous features of the applicants claims, such as splitting data using a splitting part into plural bit strings, and then processing the plural bit strings using nonlinear transformation parts, remains undisclosed or suggested when the references are combined as suggested in the Office Action.

The allegation that claims 28, 29, 32, 33, 36, 37, 42, 43, 46 and 47 are obvious in view of Matsui and DES appear to be the result of an impermissible use of hindsight. While the teachings of Kwan (The Design of the ICE Encryption Algorithm) may disclose data being broken into four parts, is not considered that Kwan when combined with DES and Matusi would yield or disclose the specific subject matter of claims 28 which require four specific routes.

15

Application No.: 09/446,525   Docket No.: 20162-00540-US
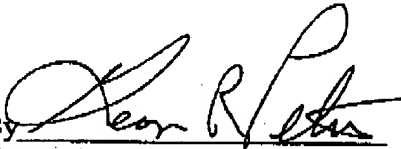
Further, the allegation that claims 30, 34, 38, 44 and 48 are obvious in light of the combined teachings of DES and Matsui are similarly believed to be the result of hindsight. The elements of these claims requiring first through fourth routes, followed by a nonlinear transformation appears unsuggested in any of the references, or any combination of the cited references.

In view of the foregoing, favorable reconsideration is believed to be in order.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 20162-00540-US from which the undersigned is authorized to draw.

Dated: November 13, 2003   Respectfully submitted,

By _____
George R. Pettit, Reg. No. 27,369
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036-3425
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant

16